UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

JEREMY ANGELLE, individually and on behalf of all others similarly situated, Plaintiff, v. GARDAWORLD CASHLINK LLC, d/b/a GARDAWORLD CASH, Defendant.	Case No. _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jeremy Angelle ("Plaintiff") brings this action on behalf of himself and all others similarly situated against Defendant GardaWorld Cashlink LLC d/b/a GardaWorld Cash ("GardaWorld" or "Defendant"). Plaintiff(s) seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from GardaWorld. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of GardaWorld's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff's and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes, resulting in an November 2023 data breach ("Data Breach") of documents and information stored on the

computer network of GardaWorld, a cash management solutions company offering cash automation for businesses.[1]

2. Defendant's data security failures allowed a targeted cyberattack in October through November 2023 to compromise Defendant's network (the "Data Breach") that contained personally identifiable information ("PII" or "Private Information") of Plaintiff and other Class Members.

3. According to notices sent to State Attorneys General, this Data Breach occurred from October 30, 2023 through November 16, 2023, and included the Private Information of approximately **39,928 individuals**, including Plaintiff and Class, although it admits that its investigation is on-going.[2]

4. Despite learning of the Data Breach in November 2023 and determining that Private Information was involved in the breach, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until March 2024.

5. On its computer network, GardaWorld holds and stores certain highly sensitive personally identifiable information, PII, of the Plaintiff and the putative Class Members, i.e., individuals who provided their highly sensitive and private information in exchange for employment or financial services.

6. GardaWorld was required to begin notifying victims of its Data Breach as soon as possible, informing them that their PII had been stolen in a data breach, yet failed to do so.

7. GardaWorld admits that an unknown actor gained access to the GardaWorld network and that its investigation also revealed the stolen data included: names, Social Security

[1] https://cash.garda.com/ (last accessed Apr. 3, 2024).
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/b259cad1-d4ba-46cf-9a2a-05ff391ebfcc.shtml (last accessed Apr. 3, 2024).

numbers, Driver's License numbers, dates of birth, and/or insurance, benefits, or other health-related information.[3]

8. As a result of GardaWorld's Data Breach, Plaintiff(s) and millions of Class Members suffered or will suffer imminently ascertainable losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

9. Based upon GardaWorld's Attorneys General notification and its Notice Letter, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff and Class Members' Private Information.

11. Plaintiff(s) bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

12. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant.

[3] *Id.* (*see* link to Notice Letter)

Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Defendant disregarded the privacy and property rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate and complete notice of the Data Breach.

14. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner, and potentially been able to mitigate the injuries to Plaintiff(s) and the Class.

15. Plaintiff's and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

16. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

17. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

20. Accordingly, Plaintiff brings this action against Defendant for negligence / negligence *per se*, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for GardaWorld's unlawful conduct.

21. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

THE PARTIES

22. Plaintiff Jeremy Angelle is and at all times relevant to this Complaint an individual citizen of the State of Louisiana, residing in Opelousa.

23. GardaWorld is a Florida limited liability company organized and headquartered in Boca Raton, Florida. GardaWorld's principal place of business is located at 2000 NW Corporate Blvd., Boca Raton, Florida 33431.

24. Defendant can be served through its registered agent at: C T Corporation System, 1200 South Pine Island Road, Plantation, Florida 33324.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class (including Plaintiff Angelle) is a citizen of a state different from Defendant.

26. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a limited liability company; it maintains its headquarters in Florida; and committed tortious acts in Florida.

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which GardaWorld has the most significant contacts.

STATEMENT OF FACTS

28. GardaWorld claims to offer "modern cash processing for consumer businesses and financial institutions, with a range of products and services that can be used a la carte or bundled into end-to-end solutions that integrate cash and digital revenue streams to enable an optimized treasury operation for any business."[4]

29. According to its website, GardaWorld's services include ATM services, cash inventory & forecasting, cash vault services, secured transportation.[5]

[4] https://cash.garda.com/why-us (last accessed Apr. 3, 2024).
[5] https://cash.garda.com/ (last accessed Apr. 3, 2024).

30. According to its Privacy Policy, GardaWorld states that it employs "appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed."[6]

31. Plaintiff and Class Members entrusted GardaWorld with highly sensitive PII, including but not limited to Social Security numbers.

32. The information held by Defendant in its computer systems or those of its customers at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

33. Upon information and belief, both Defendant and its customers made promises and representations to Plaintiff and Class Members, that the PII collected as a condition of employment, business, or financial services would be kept safe, confidential, that the privacy of that information would be maintained, and any sensitive information gathered and stored would be deleted after it was no needed for legitimate business purposes and/or no longer legally necessary to maintain.

34. Plaintiff and Class Members provided their PII to Defendant directly or indirectly through another party with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access and would make only authorized disclosures of this information.

35. Consumers, in general, demand that businesses that require highly sensitive PII will provide security to safeguard their PII, especially when Social Security numbers are involved.

36. In the course of dealings, including Plaintiff and Class Members, provided GardaWorld with all or most of the following types of Private Information:

[6] https://cash.garda.com/privacy-policy (last accessed Apr. 3, 2024).

- First and last names;
- Home addresses;
- Dates of birth;
- Social Security numbers;
- Financial information;
- Photo identification and/or driver's licenses;
- Certain health-related information
- Email addresses; and
- Phone numbers.

37. GardaWorld had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from unauthorized disclosure to third parties.

The Data Breach

38. According to the Notice Letters sent to Attorneys General and Plaintiff(s), GardaWorld first discovered suspicious activity in its systems on November 16, 2023, and "discovered that [it was] the victim of a cybersecurity incident that impacted certain administrative files stored on some of our facility systems in Florida. As soon as [it] became aware of this incident, [it] promptly took steps to secure [its] systems, launched an investigation, and engaged external cybersecurity experts to assist.[7]

39. Plaintiff's and Class members' PII was in the hands of cybercriminals for over 4 months before they were notified of the Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical. Because of this targeted,

[7] *See* Plaintiff's Notice Letter, attached as Ex. A.

intentional cyberattack, data thieves were able to gain access to and obtain data from GardaWorld that included the PII, including Social Security numbers, of Plaintiff and Class Members.

40. GardaWorld includes no details regarding the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken it has taken since the Data Breach to ensure such a breach does not occur again. To date, Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected, have no explanation of these critical facts and actions.

41. GardaWorld's notice to Plaintiff and the Class fails to inform, Plaintiff and Class Members of the Data Breach's critical details, without which they are unable to fully mitigate their own injuries resulting from the Data Breach.

42. Upon information and belief, the Private Information stored on GardaWorld's network was not encrypted.

43. Plaintiff(s)' Private Information was accessed and stolen in the Data Breach. Plaintiff reasonably believes their stolen Private Information is currently available for sale on the Dark Web because that is the modus operandi of cybercriminals who target businesses that collect highly sensitive Private Information.

44. As a result of the Data Breach, GardaWorld now encourages Class Members to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiff and Class members.

45. That GardaWorld is encouraging Plaintiff and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

46. GardaWorld had obligations created by contract, industry standards, and common law to keep Plaintiff(s)'s and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

47. GardaWorld could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII.

Defendant Acquires, Collects, and Stores PII.

48. GardaWorld acquires, collects, and stores a massive amount of personally identifiable information ("PII") of individuals who are seeking employment, financial or business services.

49. By obtaining, collecting, and using Plaintiff's and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting that PII from unauthorized or criminal disclosure.

50. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

51. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

A Data Breach was a Foreseeable Risk

52. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including GardaWorld, are well aware of the risk of being targeted by cybercriminals.

53. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

54. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[8]

55. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

56. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

57. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state

[8] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Apr. 3, 2024).

motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[9]

58. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

59. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. In a poll done on security executives, in 2020 they predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated within the next 2 years. Unfortunately, these preventable causes were expected—even then—to come from "misconfigurations, human error, poor maintenance, and unknown assets."[11]

60. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

61. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations

[9] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Apr. 3, 2024).
[10] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Apr. 3, 2024).
[11] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Apr. 3, 2024).

and the loss of critical information and data."[12] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[13]

62. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, GardaWorld failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

63. Further, GardaWorld failed to abide by its own Privacy Policy.[14]

Defendant Had a Duty to Properly Secure PII

64. At all relevant times, GardaWorld had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when GardaWorld became aware that their PII was compromised.

65. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

66. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

---

[12] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Apr. 3, 2024).

[13] *Id.*

[14] https://cash.garda.com/privacy-policy

- Maintaining a secure firewall configuration;
- Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- Monitoring for suspicious or irregular traffic to servers;
- Monitoring for suspicious credentials used to access servers;
- Monitoring for suspicious or irregular activity by known users;
- Monitoring for suspicious or unknown users;
- Monitoring for suspicious or irregular server requests;
- Monitoring for server requests for PII;
- Monitoring for server requests from VPNs; and
- Monitoring servers for requests from Tor exit nodes.

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

68. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers,

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*

fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personal Identifiable Information

69. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[17]

70. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[18]

71. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding

[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Apr. 3, 2024).

[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed Apr. 3, 2024).

payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

72. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

74. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

75. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Apr. 3, 2024).

[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Apr. 3, 2024).

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Apr. 3, 2024).

other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[22]

76. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

77. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

78. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

79. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

[22] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed Apr. 3, 2024).

80. One such example of criminals piecing together bits and pieces of compromised PII and/or PHI for profit is the development of "Fullz" packages.

81. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

82. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

83. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

84. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as dates of birth paired with Social Security numbers).

85. Moreover, GardaWorld has offered only a two-year subscription for identity theft monitoring and identity theft protection through CyEx. Its limitation is inadequate when the victims are likely to face many years of identity theft.

86. Furthermore, Defendant's credit monitoring offer and advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects

Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

87. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

88. The injuries to Plaintiff and Class Members were directly and proximately caused by GardaWorld's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

89. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and

[23] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 3, 2024).

practices for business.[24] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

91. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[25]

92. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[26]

93. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

[24]Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Apr. 3, 2024).

[25] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed Apr. 3, 2024).

[26] See FTC, Start With Security, supra.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large

amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

94. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

95. Because Class Members entrusted Defendant with their PII, Defendant had, and has, a duty to the Plaintiff and Class Members to keep their PII secure.

96. Plaintiff and the other Class Members reasonably expected that when they provide PII/PHI to Defendant directly or indirectly to GardaWorld, that Defendant would safeguard their PII.

97. GardaWorld was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff(s) and members of the Class. GardaWorld was also aware of the significant repercussions if it failed to do so. Through its own Privacy Policies, quoted above, GardaWorld acknowledges this awareness.

98. GardaWorld's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' full names, dates of birth, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant's Inadequate Security caused Concrete Injuries

99. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

100. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. Plaintiff and other individuals whose PII was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and Class Members suffered pecuniary injury.

101. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff and Class have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

102. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;

- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

103. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

104. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

105. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

106. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[27] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

---

[27] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Apr. 3, 2024).

107. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

Loss Of Time to Mitigate Risk of Identity Theft and Fraud

108. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

109. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

110. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

111. Likewise, these efforts are consistent with the advice given to Plaintiff and the Class by GardaWorld in its Notice Letters.

Data Breaches Put Consumers at an Increased Risk of Identify Theft

112. Data Breaches, such as the one experienced by GardaWorld, are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

113. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach. Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. See GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

114. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").

115. The FTC, like the GAO (see Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

116. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.

117. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

118. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

119. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their personal accounts for many years to come.

PLAINTIFF'S FACTUAL ALLEGATIONS

120. Plaintiff Jeremy Angelle is and at all times relevant to this Complaint an individual citizen of the State of Louisiana, residing in Opelousa. He received a letter from GardaWorld entitled Notice of Data Breach and dated March 22, 2024, attached as Exhibit A.

121. Plaintiff is a former employee of GardaWorld. GardaWorld required Plaintiff Angelle provide it with Plaintiff's PII and PHI. GardaWorld was provided with his personal information, including but not limited to his Social Security number.

122. Around or after April 1, 2024, Plaintiff Angelle received the Notice of Letter, which indicated that GardaWorld had known about the Data Breach for 4 months. The letter informed him that her critical PII was accessed by an unauthorized actor. The letter stated that the extracted information included his "name, Social Security number, Driver's License number, date of birth, and/or insurance, benefit, or other health-related information" but did not expand on whether additional information was stolen as well. See Notice Letter, attached as Exhibit A.

123. Plaintiff is alarmed by the amount of his Personal Information that was stolen or accessed, and even more by the fact that his Social Security number was identified as among the breach data on GardaWorld's computer system.

124. For a little over a month now, Plaintiff has been receiving many spam calls, texts, and emails each day. Prior to this time, he was receiving maybe one troublesome call and/or email per day.

125. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a social engineering attack.

126. In response to GardaWorld's Notice of Data Breach, Plaintiff has spent and will continue to be required to spend time dealing with the consequences of the Data Breach, which

will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

127. Plaintiff was notified by GardaWorld that he should enroll in a credit monitoring service to thwart identity theft and should also change his email passwords. He has been doing these actions, resulting in lost time, at the advice of GardaWorld.

128. Immediately after receiving the Notice Letter, Plaintiff spent time discussing options with a law firm, changing passwords, considers replacing his bank cards, contacted the bank about the breach, and has started to check his financial accounts for a minimum of thirty minutes per week in an effort to mitigate the damage that has been caused by GardaWorld.

129. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

130. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided GardaWorld or its customer with her PII had GardaWorld disclosed that it lacked data security practices adequate to safeguard PII.

131. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that was entrusted to GardaWorld.

132. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

133. Plaintiff reasonably believes that his Private Information may have already been sold by the cybercriminals. Had he been notified of GardaWorld's breach in a more timely manner, he could have attempted to mitigate her injuries.

134. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

135. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief remains backed up and in GardaWorld's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

136. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following Class:

> All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the Data Breach discovered by Defendants on or about November 16, 2023.

137. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

138. Also, in the alternative, Plaintiff requests additional Subclasses as necessary based on the types of PII that were compromised.

139. Plaintiff reserves the right to amend the above definition or to propose Subclasses in subsequent pleadings and motions for class certification.

140. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using and/or safeguarding their PII/PHI;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Plaintiff's and Class Members' PII;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

11) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused

by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Plaintiff in this class action is an adequate representative in that the Plaintiff has the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entireties. Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

141. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in their entirety, not on facts or law applicable only to Plaintiff.

142. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure Class Members' PII, and Defendant may continue to act unlawfully as set forth in this Complaint.

143. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

FIRST CLAIM FOR RELIEF
Negligence / Negligence *Per Se*
(On behalf of the Class)

144. Each and every allegation of the preceding paragraphs 1-145 is incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

145. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff's and Class Members' PII in its computer systems and on its networks.

146. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII.

147. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

148. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

149. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

150. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

151. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

152. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

153. Plaintiff's and Class Members' willingness to entrust Defendant and/or its customers with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

154. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiff and/or the remaining Class Members.

155. Defendant breached its general duty of care to Plaintiff and Class Members in but not necessarily limited to the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII;

b. by failing to timely and accurately disclose that Plaintiffs' and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiffs' and Class Members' PII, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

156. Defendant's willful failure to abide by these duties was wrongful, reckless and grossly negligent in light of the foreseeable risks and known threats.

157. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

158. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII/PHI.

159. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

160. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII/PHI.

161. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' PII/PHI was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

162. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

163. The damages Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

164. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses such as Defendant of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

165. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

166. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.*

167. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not

limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII is used, (iii) the compromise, publication and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

168. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

169. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Class)

170. Each and every allegation of the preceding paragraphs 1-145 is incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

171. Through their course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

172. Defendant required its customers and/or Plaintiff and Class Members directly to provide and entrust their PII to it as a condition of obtaining Defendant's services.

173. Plaintiffs would not have provided their PII to Defendant without Defendant's agreement to protect it.

174. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

175. As a condition of being direct or indirect customers/clients of Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

176. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant in exchange for, amongst other things, the protection of their PII.

177. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

178. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

179. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of the Class)

180. Each and every allegation of the preceding paragraphs 1-145 is incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

181. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of the provision of their PII, and Defendant would be unable to engage in its regular course of business without that PII.

182. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

183. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a

reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

184. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

185. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

186. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

187. Plaintiff and Class Members have no adequate remedy at law.

188. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and/or will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity how their PII is used, (iii) the compromise, publication, and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft, (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect PII in their continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PII compromised as a result of the Data Breach for the remainder of Plaintiffs' and Class Members' lives.

189. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

190. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FOURTH CLAIM FOR RELIEF
Declaratory Judgment
(On behalf of the Class)

191. Each and every allegation of the preceding paragraphs 1-145 is incorporated in this Cause of Action with the same force and effect as though fully set forth herein.

192. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

193. An actual controversy has arisen in the wake of Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII.

194. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff and Class will continue to suffer injury as a result of the compromise of their PII and

remain at imminent risk that further compromises of their PII will occur in the future.

195. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under common law, Section 5 of the FTC Act, and various state statutes;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII/PHI.

196. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

197. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach on Defendant's systems. The risk of another such breach is real, immediate and substantial. If another breach occurs to Defendant, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

198. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant is subject to another data breach, Plaintiff and Class Members will likely be subjected to fraud, identify theft and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

199. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach on Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PII would be further compromised.

RELIEF SOUGHT

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed Class, respectfully requests the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed Class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge Plaintiff's and Class Members' PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII/PHI;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII/PHI on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII/PHI, as well as protecting Plaintiff's and Class Members' PII/PHI;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: April 3, 2024

Respectfully Submitted,

/s/ Jeff Ostrow

Jeff Ostrow, FBN 121452
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 332.4200
ostrow@kolawyers.com